NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.15.2017
P/17/062

02266617

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku
ul. Akademicka 4, 15-267 Białystok
T +48 85 874 81 00, F +48 85 874 81 33
lbi@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	P/17/062 – Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w województwie podlaskim
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontrolerzy	Beata Palinowska – starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/168/2017 z 28 listopada 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Urząd Miejski w Szepietowie, ul. Główna 6, 18-210 Szepietowo (dalej: „Urząd")
Kierownik jednostki kontrolowanej	Robert Lucjan Wyszyński – Burmistrz Szpietowa[1] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[2]

Ocena ogólna

Najwyższa Izba Kontroli ocenia negatywnie zapewnienie przez Urząd właściwej ochrony elektronicznych zasobów informacyjnych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem[3].

Uzasadnienie oceny ogólnej

Stwierdzono bowiem m.in. następujące nieprawidłowości:

- wbrew postanowieniom § 20 ust. 2 pkt. 12 lit. a rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[4], żaden komputer pracujący w sieci LAN Urzędu nie posiadał aktualnego systemu operacyjnego,
- nie zapewniono odpowiedniego mechanizmu kontroli dostępu do danych, gdyż nie analizowano i nie zabezpieczono przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów, a jednemu pracownikowi nie nadano indywidualnego loginu i hasła, mimo że przetwarzał dane w systemach Urzędu,
- pracownikom zaangażowanym w proces przetwarzania informacji nie zapewniono szkoleń, uwzględniających zagadnienia z zakresu zagrożenia bezpieczeństwa informacji,
- nie odebrano niezwłocznie dostępu do systemu zawierającego dane osobowe pracownikowi, z którym rozwiązano stosunek pracy, a innemu pracownikowi nadano uprawnienia w systemie informatycznym niezgodne z zakresem czynności, co naruszało przepisy § 20 ust. 2 pkt. 4 i 5 rozporządzenia KRI,
- nie były wykonywane kopie bezpieczeństwa danych na serwerze, a kopie systemów informatycznych służących do przetwarzania danych osobowych były wykonywane niezgodnie z Instrukcją zarządzania systemem informatycznym[5],
- dziesięć zbiorów danych nie zostało zgłoszonych do rejestru zbiorów danych prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych[6], a w trzech zbiorach gromadzono dane w zakresie szerszym niż zgłoszony.

---

[1] Funkcję Burmistrza Szepietowa pełni od 1 grudnia 2014 r.
[2] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.
[3] Okres objęty kontrolą: od 1 stycznia 2016 r. do dnia zakończenia czynności kontrolnych oraz działania wcześniejsze mające wpływ na kontrolowaną działalność.
[4] Dz. U. z 2016 r. poz. 113, ze zm. Rozporządzenie zwane dalej: „rozporządzeniem KRI".
[5] Dalej: „Instrukcja zarządzania".
[6] Dalej: „GIODO".

III. Opis ustalonego stanu faktycznego

Opis stanu faktycznego

1. Skuteczność przyjętych rozwiązań dotyczących zabezpieczenia dostępu do poszczególnych systemów informatycznych i usług sieciowych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem danych

1.1. W Urzędzie do gromadzenia i przetwarzania danych osobowych były wykorzystywane następujące systemy informatyczne: SmartDoc, ŹRÓDŁO, SELWIN, USCWIN, Budżet, Kadry i Płace, Kasa, Podatki, Księgowość zobowiązań, Auta, Rejestr VAT, FISKUS, Egzekucje, Płatnik. Przyjęto, zgodnie z § 6 ust. 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[7], wysoki poziom zabezpieczeń, w związku z tym, że wszystkie stanowiska komputerowe, na których znajdowały się systemy służące do przetwarzania danych osobowych (poza przeznaczonymi do obsługi systemu ŹRÓDŁO) posiadały dostęp do Internetu. (dowód: akta kontroli str. 93)

W trakcie oględzin wszystkich 28 stanowisk komputerowych Urzędu (w tym dwóch służących do obsługi systemu ŹRÓDŁO oraz jednego działającego poza siecią LAN) stwierdzono, że na 26 użytkownicy nie posiadali uprawnień administratora systemu operacyjnego, w każdym przypadku dostęp do tego systemu był zabezpieczony loginem i hasłem, konfiguracja komputera na wszystkich stanowiskach umożliwiała uaktywnienie się wygaszacza ekranu, a powrót do systemu wymagał podania loginu i hasła dostępu. Na jednym (z 26) komputerze system operacyjny był aktualny. Na trzech komputerach zainstalowano system Windows XP (jeden komputer służył do obsługi systemu, w którym przetwarzane były dane osobowe). Program antywirusowy był aktualny na 26 (z 28) stanowiskach.

Nieprawidłowości w powyższym zakresie opisano szerzej w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 8-28)

We wrześniu 2016 roku w Urzędzie była przeprowadzona analiza ryzyka utraty integralności, dostępności lub poufności informacji. W wyniku analizy zidentyfikowane zostały potencjalne zagrożenia oraz ryzyko ich wystąpienia. W 2017 roku nie przeprowadzono takiej analizy, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności"
(dowód: akta kontroli str. 198-203, 219-220)

Na 25 (z 26) komputerach pracownicy przetwarzający dane osobowe posiadali uprawnienia użytkownika systemu nadane przez Administratora Systemu Informatycznego (dalej: „ASI"). 24 (z 25) pracowników posiadało własny login i hasło (nieposiadanie przez jednego pracownika loginu i hasła szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości"). (dowód: akta kontroli str. 8-28)

Nadane uprawnienia dziewięciu (z 10) pracowników były adekwatne do realizowanych zadań wynikających z ich zakresów czynności, stosownie do przepisu § 20 ust. 2 pkt 4 rozporządzenia KRI. Hasła dostępu dwóch (z 26) użytkowników spełniały wymagania określone w obowiązującej w Urzędzie Instrukcji Zarządzania Systemem Informatycznym (dalej: „Instrukcja zarządzania") oraz w załączniku do rozporządzenia w sprawie dokumentacji i warunków technicznych. Nieprawidłowości dotyczące zmiany uprawnień oraz niespełnienia wymogów w zakresie hasła dostępu do systemu operacyjnego, szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 179-181)

1.2. W Urzędzie nie wdrożono polityki gromadzenia, zabezpieczania i automatycznej analizy logów. Nie prowadzono też zbiorczego rejestru dostępu do systemu w formie papierowej lub elektronicznej. Informacje o dostępie były zapisywane indywidualnie dla każdego klienta domenowego, a tryb zarządzania logami (ich zawartość i czas

[7] Dz. U. Nr 100, poz. 1024 ze zm. Rozporządzenie zwane dalej: „rozporządzeniem w sprawie dokumentacji i warunków technicznych".

systemu[8]. Logi związane z pracą systemu nie były jednak analizowane. Logi routera, serwera i aplikacji na nim działających były zabezpieczone przed dostępem użytkowników systemu, jednak informacje zawarte w logach nie były przetwarzane automatycznie przez ASI. Szerzej nieprawidłowości w zakresie monitorowania dostępu do systemu opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 187-193)

1.5. W Urzędzie, zgodnie z § 20 ust. 2 pkt 7 lit. c rozporządzenia KRI, zapewniono środki uniemożliwiające nieautoryzowany dostęp na poziomie systemów operacyjnych (zastosowano wymuszenie okresowej zmiany hasła), usług sieciowych i urządzeń serwerowni, poprzez zabezpieczenie hasłem. Sieć Wi-FI była odseparowana fizycznie od sieci LAN, a dostęp do niej zabezpieczony był hasłem, które było udostępniane wybranym osobom. (dowód: akta kontroli str.187-193)

1.6. W przyjętych procedurach wewnętrznych dotyczących ochrony danych osobowych nie uregulowano kwestii związanych z wykorzystaniem do pracy sprzętu niebędącego własnością Urzędu. (dowód: akta kontroli str. 36-65)

Konfiguracja sieciowa umożliwiała podłączenie do infrastruktury jednostki sprzętu (laptopy, telefony, tablety) niestanowiącego własności pracodawcy. Informacje o podłączeniu do komputerów nośników pamięci były domyślnie zapisywane w logach systemu komputerowego, jednak informacja o podłączeniu nie była na bieżąco analizowana i zabezpieczana w sposób trwały. Dostęp do zasobów sieciowych uwierzytelniany był na poziomie użytkownika. Nie przewidziano zdalnego dostępu do zasobów sieci lokalnej przez pracowników. (dowód: akta kontroli str. 187-193)

Na 15 komputerach zainstalowano aplikację pulpitu zdalnego TeamViewer, z której korzystali pracownicy firmy ZETO Białystok podczas realizacji prac serwisowych oraz ASI. Dostęp pracowników tej firmy nie był objęty kontrolą ASI, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 8-28, 187-193)

1.7. Od 1 stycznia 2016 r. do 1 grudnia 2017 r. nie wystąpiły przypadki wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji.

(dowód: akta kontroli str. 219-220)

Pracowników użytkujących komputery przenośne zobowiązano do zachowania szczególnej ostrożności podczas ich transportowania, przechowywania i użytkowania. W Urzędzie użytkowany był jeden komputer przenośny, który nie miał szyfrowanego dysku, a dostęp do systemu operacyjnego był zabezpieczony hasłem. Nie przewidziano zdalnego dostępu pracowników do zasobów sieci lokalnej (komputer nie był użytkowany poza siedzibą Urzędu). (dowód: akta kontroli str. 27-28, 52-65, 187-193)

1.9. W umowach związanych z serwisem i aktualizacją programów wykorzystywanych do gromadzenia i przetwarzania danych osobowych (m.in. Selwin, USCWin, Sputnik, Kadry i Płace, Kasa, Podatki, Rejestr VAT, Przelewy) zawarte były zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, co było zgodne z § 20 ust. 2 pkt. 10 rozporządzenia KRI. Obejmowały one w szczególności zobowiązanie do: [1] zapewnienia aktualizacji oprogramowania; [2] przestrzegania przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[9]; [3] zachowania w tajemnicy informacji uzyskanych w trakcie realizacji umów. (dowód: akta kontroli str. 100-141)

1.10. 23 komputery (z 25 podłączonych do sieci LAN Urzędu) były zabezpieczone przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, dedykowanym do tego celu oprogramowaniem. Komputery te posiadały aktualne wersje aplikacji zabezpieczających. Dwa komputery nie miały zainstalowanego aktualnego oprogramowania, co szerzej opisano w dalszej części wystąpienia pokontrolnego w sekcji „Ustalone nieprawidłowości".

---

[8] Ruter był administrowany poza Urzędem, w związku z tym nieznane były jego ustawienia w zakresie zarządzania logami.
[9] Dz. U. z 2016 r. poz. 922.

Dostęp do sieci lokalnej kontrolowany był przez firewall zainstalowany na routerze CISCO. Było to zgodne z pkt III załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych. (dowód: akta kontroli str. 8-28, 187-193)

1.11. Urząd wykupił usługę hostingu strony internetowej, domenę internetową oraz pocztę elektroniczną w podmiocie zewnętrznym. Dane poczty przechowywano na serwerze usługodawcy, który był również ich administratorem. W § 5 pkt 4 regulaminu podmiot realizujący usługę poinformował o zakazie rozpowszechniania szkodliwego oprogramowania bądź wiadomości typu Spam. (dowód: akta kontroli str. 142-147)

1.12. W Urzędzie nie były wykonywane kopie bezpieczeństwa baz danych. Kopie zapasowe były wykonywane przy okazji aktualizacji aplikacji specjalistycznych wykorzystywanych do obsługi Urzędu, a ich częstotliwość i sposób przechowywania nie była zgodna z uregulowaniami obowiązującymi w Urzędzie. Szerzej nieprawidłowości w tym zakresie opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 52-65, 187-193)

1.13. Pracownicy Urzędu dysponowali możliwością ściągania aplikacji i plików wykonalnych, natomiast nie posiadali uprawnień do instalowania ich na stacjach komputerowych, do których mieli dostęp. Uprawnienia do konfiguracji systemów operacyjnych komputerów działających w sieci LAN posiadał tylko administrator. (dowód: akta kontroli str. 187-193)

Na trzech komputerach były użytkowane systemy operacyjne Windows XP, dla których producent zakończył wsparcie techniczne. Wszystkie były podłączone do sieci wewnętrznej, a jeden służył do obsługi systemu, w którym były przetwarzane dane osobowe (komputer ten nie posiadał również aktualnego oprogramowania chroniącego przed szkodliwym oprogramowaniem, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości"). (dowód: akta kontroli str. 8-28)

W Urzędzie prowadzona była ewidencja oprogramowania dopuszczonego do użytkowania oraz wykaz użytkowanego sprzętu komputerowego. Rejestry te nie były aktualizowane na bieżąco i nie obejmowały danych dotyczących systemów operacyjnych zainstalowanych na komputerach, a także danych dotyczących konfiguracji oprogramowania, co szerzej opisano w pkt. 3.2. wystąpienia pokontrolnego. (dowód: akta kontroli str. 93, 99)

1.14. Systemy operacyjne zainstalowane na komputerach wchodzących w skład sieci wewnętrznej Urzędu nie były aktualizowane, a aplikacja bezpieczeństwa była aktualna na 23 (z 25) komputerach. Szerzej nieprawidłowości w zakresie niezapewnieniu aktualizacji oprogramowania opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 8-28)

1.15. W Urzędzie nie były opracowane regulacje wewnętrzne w zakresie dokonywania płatności drogą elektroniczną. Płatności były dokonywane poprzez stronę internetową banku. Po sprawdzeniu dokumentu pod względem merytorycznym i formalno-rachunkowym oraz zatwierdzeniu go do wypłaty / przelewu wyznaczony pracownik sporządzał szablon przelewu, który był zatwierdzany przez dwie uprawnione osoby z wykorzystaniem narzędzi uwierzytelniających. (dowód: akta kontroli str. 148-167)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono niżej wymienione nieprawidłowości.

1. Jeden (z 26) pracownik nie posiadał nadanego loginu i hasła do systemu informatycznego. Korzystał z loginu i hasła udostępnionego przez innego pracownika. Zgodnie z częścią A pkt II załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych w systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych, a jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator i dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

   ASI wyjaśnił, że: *„Nie byłem świadomy, ze taka sytuacja może mieć miejsce i dla Pani (...) potrzebny jest dostęp do komputera. Użytkownik został pouczony o bezwzględnym*

zakazie udostępniania haseł osobom trzecim, a Pani (...) w dniu 8 stycznia 2018 r. założono indywidualne konto użytkownika". (dowód: akta kontroli str. 19, 227, 284-291)

2. Oględziny komputerów wykazały, że hasła dostępu do systemu operacyjnego 24 (z 26) użytkowników nie spełniało wymogów określonych w Instrukcji Zarządzania Urzędu oraz w cz. B pkt VIII załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych, w odniesieniu do określonej w tych przepisach liczby znaków (w przypadku 24 użytkowników) i poziomu złożoności (20 użytkowników).

   ASI wyjaśnił, że: „*Polityka bezpieczeństwa haseł była skonfigurowana na serwerze zgodnie z wymogami przepisów prawa (...) dodatkowo serwer wymuszał comiesięczną zmianę haseł (...). Jednak (...) polityka ta nie działała w sposób prawidłowy, gdyż błędnie na kontach wszystkich użytkowników była zaznaczona opcja, że „hasło nigdy nie wygasa" Błąd ten został usunięty w dn. 28 grudnia 2017 r. i została wymuszona zmiana haseł dla wszystkich użytkowników na prawidłowe*".

   Nieprawidłowość została usunięta w trakcie kontroli.

   (dowód: akta kontroli str. 8-28, 284-291)

3. Cofnięcie uprawnień do systemu SmartDoc pracownikowi, którego stosunek pracy wygasł 28 października 2017 r nastąpiło dopiero w trakcie kontroli (8 stycznia 2018 r.), tj. z dwumiesięcznym opóźnieniem. Natomiast inny pracownik posiadał dostęp do systemu informatycznego Kadry i płace niezgodny z upoważnieniem do przetwarzania danych osobowych, udzielonym przez Administratora Danych Osobowych (dalej: „ADO").

   Było to sprzeczne z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI. Zgodnie z tymi przepisami zarządzanie bezpieczeństwem informacji realizowane jest poprzez podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych zadań oraz obowiązków, mających na celu zapewnienie bezpieczeństwa informacji, oraz poprzez bezzwłoczną zmianę uprawnień w przypadku zmiany zadań osób zaangażowanych w proce przetwarzania informacji.

   ASI wyjaśnił, że: „*W systemie SmartDoc nie zostały zabrane uprawnienia na skutek przeoczenia. Dla Pani (...) zabrano dostęp do systemu Kadry i płace w dniu 8 stycznia 2018 r., a pozostałym dwóm pracownikom udzielono w dniu 4 stycznia 2018 r. poprawnych upoważnień*". (dowód: akta kontroli str. 6-7, 179-180, 284-291, 354)

4. W Urzędzie nierzetelnie monitorowano dostęp do informacji, bowiem nie było wdrożonej polityki gromadzenia, zabezpieczania i automatycznej analizy logów oraz nie prowadzono zbiorczego rejestru dostępu do systemu, a informacje zawarte w logach nie były przetwarzane automatycznie przez ASI. Logi zapisywane na końcówkach klienckich nie były zabezpieczone przed modyfikacją i zniszczeniem, a informacje o podłączeniu do komputerów nośników pamięci nie były trwale zabezpieczane.

   Ponadto ASI nie nadzorował korzystania przez pracowników firmy ZETO (podczas realizacji prac serwisowych) z aplikacji pulpitu zdalnego TeamViewer.

   Stanowiło to naruszenie § 20 ust. 2 pkt. 7 lit. a rozporządzenia KRI, stosownie do którego zarządzanie bezpieczeństwem informacji realizowane jest przez zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, poprzez monitorowanie dostępu do informacji.

   ASI wyjaśnił, że: „*Nie byłem świadomy, że zbiorczy rejestr trzeba prowadzić. Urząd nie posiada blokady portów USB, jest jedynie włączone skanowanie urządzeń wymiennych przez program antywirusowy. Zastosowano zabezpieczenie organizacyjne w postaci szkolenia oraz wprowadzenia polityki bezpieczeństwa informacji, która zakazuje korzystania z nośników zewnętrznych bez zgody Administratora Danych. Po remoncie budynku Urzędu Miejskiego, planowany jest zakup nowego serwera do zarządzania siecią i przechowywania danych, który będzie miał możliwość zdalnej blokady urządzeń wymiennych. Firma ZETO używa aplikacji TeamViewer do drobnych prac konserwacyjnych programów (...) związanych głównie z pracą użytkowników, dlatego odbywa się to na zasadzie udostępniania pulpitu z uprawnieniami użytkownika, który kontroluje co wykonuje konsultant. Firma ZETO wszystkie poważniejsze*

aktualizacje oprogramowania wykonuje na miejscu przynajmniej raz w kwartale przy użyciu wydzielonego konta o nazwie Serwis lub jeżeli istnieje konieczność ingerencji w pliki systemowe, aktualizacja odbywa się w mojej obecności na koncie z prawami administratora." (dowód: akta kontroli str. 8-28, 189-193, 284-291)

5. W Urzędzie – wbrew postanowieniom § 20 ust. 2 pkt. 12 lit. a rozporządzenia KRI – nie zapewniono aktualizacji systemu operacyjnego zainstalowanego na 25 (z 26) komputerach użytkowanych w Urzędzie (na wszystkich działających w sieci LAN). Niektóre z nich nie były aktualizowane od momentu instalacji, na trzech komputerach był zainstalowany system operacyjny Microsoft Windows XP, dla którego producent zakończył wsparcie, a na dwóch nie była zainstalowana aplikacja bezpieczeństwa. Było to sprzeczne z § 20 ust. 2 pkt 12 lit a rozporządzeni KRI. Zgodnie z tym przepisem zarządzanie bezpieczeństwem informacji realizowane jest poprzez zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na dbałości o aktualizację oprogramowania.

   ASI wyjaśnił, że: *„Proces aktualizacji systemów operacyjnych zarządzany był przez serwer WSUS, który miał za zadanie pobierać wszystkie wymagane aktualizacje i rozsyłać je po stacjach roboczych. Obecnie proces aktualizacji nie działa prawidłowo z nieznanych powodów, prawdopodobnie jest w tym przypadku jakiś konflikt wersji systemów operacyjnych, gdyż na wszystkich stacjach roboczych jest Windows 7 lub wyższy, a na serwerze jest Windows Server 2003. Aktualizacji nie da się też wykonać ręcznie, gdyż polityki domenowe na to nie zezwalają. W tym roku jest planowana wymiana starego serwera na nowy, pracujący w najnowszym środowisku Windows Server 2016 i problem ten zostanie rozwiązany. W planach na bieżący rok jest kasacja komputerów z systemami Windows XP, gdyż komputery te nie nadają się już do aktualizacji na nowszą wersję systemu Windows, bo mają ponad 10 lat. Tymczasowo jeszcze do czasu kasacji zainstalowano w trakcie kontroli brakujące programy antywirusowe na tych stanowiskach".* (dowód: akta kontroli str. 8-28, 284-291)

6. Nie była wykonywana kopia bezpieczeństwa serwera. Kopie systemów informatycznych służących do przetwarzania danych osobowych były zaś wykonywane z częstotliwością mniejszą niż wskazana w Instrukcji zarządzania. W 2016 roku nie były wykonane kopie w czerwcu i od sierpnia do października, a w 2017 roku – w lutym, marcu, od lipca do września i w listopadzie. Zgodnie z pkt 6 Instrukcji zarządzania kopie zapasowe danych osobowych przetwarzanych w systemach informatycznych oraz serwera powinny być wykonywane raz w miesiącu oraz nagrywane na nośnik zewnętrzny.

   ASI wyjaśnił, że: *„Kopie bezpieczeństwa nie były wykonywane ze względu na brak wolnej przestrzeni dyskowej w Urzędzie, były zrobione tylko raz po pełnej konfiguracji komputerów. Kopie systemów są robione na poszczególnych stanowiskach. Jestem świadomy, że kopie były wykonywane i testowane w sposób niezgodny z istniejącymi regulacjami. Po 10 stycznia br. Urząd będzie w posiadaniu specjalistycznego sprzętu i oprogramowania do ciągłego wykonywania kopii bezpieczeństwa aplikacji i systemów."*
   (dowód: akta kontroli str. 57-58, 189-193, 238-245, 284-291)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że w Urzędzie nie były przeprowadzane w 2017 roku okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji, mimo wymogu określnego § 20 ust. 2 pkt 3 rozporządzenia KRI. Analiza taka była przeprowadzona ostatnio 9 września 2016 r.

ASI wyjaśnił, że: *„Nie byłem świadomy, że trzeba przeprowadzać okresowe analizy ryzyka utraty integralności, dostępności i poufności informacji"*.
(dowód: akta kontroli str. 198-203, 219-220, 284-291)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie skuteczność przyjętych w Urzędzie rozwiązań dotyczących zabezpieczenia dostępu do poszczególnych systemów informatycznych i usług sieciowych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem danych.

Opis stanu faktycznego

2. Dokumentacja i procedury dotyczące ochrony danych

2.1. Urząd zgłosił GIODO do zarejestrowania 32 zbiory danych osobowych, z których zarejestrowanych zostało 31 (Urząd nie uzyskał potwierdzenia rejestracji jednego zbioru). Zarejestrowane zostały w szczególności następujące zbiory: [1] *Ochrona ludności i sprawy obronne*; [2] *Ewidencja ludności i dowody osobiste*; [3] *Podatki*; [4] *Użytkownicy wieczyści i dzierżawcy*; [5] *Wykaz dzieci uczęszczających do niepublicznych przedszkoli*; [6] *Ewidencja wniosków o leczenie odwykowe*; [7] *Ewidencja najmów i wynajmów lokali mieszkalnych i użytkowych*; [8] *Ewidencja dowożonych uczniów niepełnosprawnych*; [9] *Akta stanu cywilnego*; [10] *Rejestr skarg i wniosków*. W okresie objętym kontrolą Urząd nie występował do GIODO o wykreślenie z rejestru zbiorów danych osobowych.

(dowód: akta kontroli str. 250-267)

Nie zostało zgłoszonych dziesięć zbiorów danych osobowych: *Rejestr oświadczeń majątkowych radnych, Rejestr oświadczeń majątkowych pracowników, Monitoring wizyjny, Ewidencja Działalności Gospodarczej, Karta dużej rodziny, Rejestr VAT, Wnioski o nadanie numeru porządkowego nieruchomości, Rejestr sołtysów, Ewidencja podziałów nieruchomości* i *Zwrot podatku akcyzowego na paliwo*, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 250-267, 306-352, 380)

Zgłoszenia zbiorów danych do rejestracji zawierały większość elementów określonych w art. 41 ust 1 ustawy o ochronie danych, tj. wniosek o wpisanie zbioru do rejestru zbiorów danych osobowych; oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania; podstawę prawną upoważniającą do prowadzenia zbioru; cel przetwarzania danych; opis kategorii osób, których dane dotyczą oraz zakres przetwarzanych danych; sposób zbierania oraz udostępniania danych; informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane; opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36 – 39 powołanej ustawy; a w przypadku zbiorów gromadzonych i przetwarzanych w systemach informatycznych informację o sposobie wypełnienia warunków technicznych i organizacyjnych, określonych w przepisach, o których mowa w art. 39a ustawy i informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego.

Dziesięć (z 32 zgłoszeń) nie zawierało numeru identyfikacyjnego administratora danych osobowych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 250-267)

2.2. Burmistrz Miasta nie skorzystał z możliwości wyznaczenia Administratora Bezpieczeństwa Informacji. Upoważnieniem nr 1 z 24 marca 2015 r. wyznaczył Koordynatora Ochrony Danych Osobowych (dalej: „KODO"), któremu powierzył realizację zadań, m.in.: aktualizowanie polityki bezpieczeństwa, nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane były dane osobowe, prowadzenie ewidencji systemów informatycznych, w których przetwarzane były dane osobowe, prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych, prowadzenie rejestru zbiorów danych osobowych, zgłaszanie zbiorów danych do GIODO, prowadzenie rejestru z wykonania kopii zapasowych. (dowód: akta kontroli str. 96-98)

2.3. Burmistrz, jako administrator danych osobowych, wywiązał się z części obowiązków określonych w art. 36a ust. 2 pkt. 1 ustawy o ochronie danych osobowych. Nadzorował opracowywanie i aktualizowanie dokumentacji opisującej przetwarzanie danych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych. Osoby upoważnione do przetwarzania danych osobowych zostały zapoznane z przepisami o ich ochronie. Nie sprawdzano zgodności przetwarzania danych osobowych z tymi przepisami, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 36-37, 85-89, 194-197, 219-220)

W Urzędzie był prowadzony rejestr przetwarzanych zbiorów danych, który obejmował 31 zbiorów. Zawierał on nazwy zbiorów oraz oznaczenie ADO, cel przetwarzania danych, opis kategorii osób, których dane dotyczą, zakres przetwarzanych danych oraz sposób zbierania i udostępniania danych. (dowód: akta kontroli str. 67-69)

2.4. W Urzędzie prowadzona była ewidencja osób upoważnionych do przetwarzania danych osobowych, która obejmowała wszystkich pracowników jednostki. Zawierała ona elementy określone w art. 39 ust. 1 pkt. 1 i 2 ustawy o ochronie danych osobowych, tj. imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz identyfikator użytkownika w systemie informatycznym. W ewidencji nie odnotowano zakresu upoważnieni, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 3-5, 83-84)

Burmistrz posiadał aktualne upoważnienie do przetwarzania danych w Systemie Rejestrów Państwowych, wydane 11 grudnia 2016 r. przez Ministra Cyfryzacji. Urząd przekazał, 3 lutego i 9 grudnia 2015 r. do Ministra Cyfryzacji wykaz pracowników upoważnionych do przetwarzania danych gromadzonych w ww. systemie.

(dowód: akta kontroli str. 168-171)

Zakres upoważnień 22 (z 30) pracowników Urzędu do przetwarzania danych osobowych był zgodny z realizowanymi przez nich zadaniami. W ośmiu zaś przypadkach był inny niż wynikający z przydzielonych im zakresów czynności. Szerzej nieprawidłowości w zakresie upoważniania pracowników opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 223-226)

W pkt 8 ppkt 24 – 25 i 27 Polityki Bezpieczeństwa Informacji (dalej: „Polityka bezpieczeństwa") Urzędu uregulowano procedurę udostępniania danych osobowych oraz odnotowywania informacji o tym zdarzeniu, a także kwestię związaną z obowiązkiem zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone. (dowód: akta kontroli str. 36-51)

2.5. W Urzędzie nie były wydawane wewnętrzne akty prawne dotyczące ochrony danych osobowych, poza opisanymi w pkt. 2.10. wystąpienia pokontrolnego.

(dowód: akta kontroli str. 219-220)

2.6. Pracownika Urzędu zatrudnionego na stanowisku informatyka powołano, na podstawie upoważnienia z 24 marca 2015 r., na stanowisko ASI.

(dowód: akta kontroli str. 94-95)

2.7. Wewnętrzny audyt bezpieczeństwa informacji był przeprowadzony w Urzędzie 9 września 2016 r. W raporcie z audytu określono m.in. potrzeby: zewidencjonowania zbiorów danych osobowych prowadzonych w Urzędzie, określenia szczegółowego zakresu upoważnień dla pracowników oraz uzupełnienia dokumentacji obowiązującej w Urzędzie o opis struktury oraz powiązania dla poszczególnych zbiorów danych. Zalecenia te zostały zrealizowane. Kolejnego audytu Urząd nie przeprowadził, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 36-93, 204-220)

2.8. W okresie objętym kontrolą pracownikom Urzędu zaangażowanym w proces przetwarzania informacji nie zapewniono szkoleń z zakresu sposobu postępowania wobec zagrożeń informatycznych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Pracownicy Urzędu od listopada 2016 r. do listopada 2017 r. uczestniczyli w szkoleniu on-line z zakresu ochrony danych osobowych, które obejmowało m.in.: podstawy prawne ochrony danych osobowych, zabezpieczenie danych, dokumentację przetwarzania danych oraz planowane zmiany w zakresie ochrony danych osobowych.

(dowód: akta kontroli str. 219-220, 390-393)

2.9. W okresie objętym kontrolą w Urzędzie nie były przeprowadzane zewnętrzne kontrole w zakresie bezpieczeństwa danych osobowych. Nie wpływały również skargi związane z nieuprawnionymi przypadkami ujawnienia danych osobowych.

(dowód: akta kontroli str. 219-220)

2.10. Burmistrz, zarządzeniem nr 179A/2016 z 29 listopada 2016 r., wprowadził dokumentację związaną z przetwarzaniem danych osobowych: Politykę bezpieczeństwa oraz Instrukcję zarządzania. (dowód: akta kontroli str. 36-53, 59-79, 194-195)

Polityka bezpieczeństwa zawierała wszystkie elementy określone w § 4 rozporządzenia w sprawie dokumentacji i warunków technicznych: [1] wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, [2] wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, [3] opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, [4] sposób przepływu danych pomiędzy poszczególnymi systemami, [5] określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. (dowód: akta kontroli str. 36-93)

Instrukcja zarządzania zawierała wszystkie elementy określone w § 5 rozporządzenia w sprawie dokumentacji i warunków technicznych: [1] procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności; [2] stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem; [3] procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu; [4] procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania; [5] sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych danych; [6] sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, [7] opis procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.
(dowód: akta kontroli str. 36-93)

W Instrukcji zarządzania wprowadzony został wysoki poziom bezpieczeństwa (wszystkie urządzenia systemów informatycznych związane z przetwarzaniem danych osobowych były połączone z siecią publiczną), co odpowiadało wymaganiom określonym w § 6 rozporządzenia w sprawie dokumentacji i warunków technicznych. Zapisy Instrukcji Zarządzania odpowiadały wymogom wskazanym w załączniku do rozporządzenia w sprawie dokumentacji i warunków technicznych. (dowód: akta kontroli str. 59-79)

Przyjęte w Urzędzie regulacje odnosiły się do ochrony danych osobowych i nie zawierały wszystkich elementów określonych § 20 ust. 1 rozporządzenia KRI, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 36-93, 219-220)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono niżej wymienione nieprawidłowości.

1. Urząd nie zgłosił do rejestracji GIODO dziesięciu zbiorów danych osobowych: *Rejestr oświadczeń majątkowych radnych, Rejestr oświadczeń majątkowych pracowników, Monitoring wizyjny, Ewidencja Działalności Gospodarczej, Karta dużej rodziny, Rejestr VAT, Ewidencja numeracji porządkowej nieruchomości, Rejestr sołtysów, Ewidencja podziałów nieruchomości, Zwrot podatku akcyzowego za paliwo*. Było to niezgodne z art. 40 ustawy o ochronie danych osobowych, zobowiązującym administratora danych do zgłoszenia zbioru danych do rejestracji GIODO.

   Burmistrz wyjaśnił, że nie zgłoszono zbiorów danych na skutek niedopatrzenia. W trakcie kontroli dokonano zgłoszenia zbiorów danych do GIODO.
   (dowód: akta kontroli str. 237-238, 250-267, 292-296, 306-352, 380)

2. Dziesięć (z 32) zgłoszeń zbiorów danych do GIODO nie zawierało numeru identyfikacyjnego, wymaganego art. 41 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

   Sekretarz wyjaśnił to przeoczeniem. (dowód: akta kontroli str. 253-267, 299)

3. Nie dokonywano sprawdzenia zgodności przetwarzanych w Urzędzie danych osobowych z przepisami o ich ochronie, mimo takiego wymogu określonego w art. 36a ust. 2 pkt 1 lit. a w związku z art. 36 b ustawy o ochronie osobowych. Zgodnie z tym przepisem, w przypadku niepowołania ABI jego zadania dotyczące sprawdzanie

zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych wykonuje ADO.

Burmistrz wyjaśnił, że: *„Na skutek przeoczenia nie były przeprowadzane sprawdzenia zgodności danych osobowych przetwarzanych w Urzędzie z przepisami o ich ochronie"*.

(dowód: akta kontroli str. 219-220, 297-298)

4. Prowadzona w Urzędzie ewidencja osób upoważnionych do przetwarzania danych, wbrew wymogom art. 39 ust. 1 pkt 2 ustawy o ochronie danych osobowych, nie zawierała zakresu upoważnienia do przetwarzania danych osobowych.

   Burmistrz Miasta wyjaśnił, że wynikało to z przeoczenia.

   (dowód: akta kontroli str. 83-84, 297-298)

5. Zakres upoważnień do przetwarzania danych osobowych ośmiu (z 30) pracowników nie był zgodny z realizowanymi przez nich obowiązkami. Udzielono bowiem upoważnień do przetwarzania danych osobowych dwóm pracownikom zatrudnionym na stanowisku sprzątaczki, którym należało udzielić nie upoważnienia, lecz zgody na przebywanie w obszarze przetwarzania danych osobowych poza godzinami pracy Urzędu, stosownie do cz. A. pkt I ust. 2 załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych. Pięciu pracowników posiadało zaś dostęp do zbiorów danych (wynikający z realizowanych przez nich czynności) w zakresie szerszym niż udzielone upoważnienia, a w upoważnieniu kolejnego – nie określało zbiorów danych, do których pracownik ten może mieć dostęp.

   Stanowiło to naruszenie § 20 ust. 2 pkt 4 rozporządzenia KRI, stosownie do którego zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.

   Burmistrz wyjaśnił, że zakresy czynności pracowników zostały zmienione w trakcie kontroli oraz że cofnięto upoważnienia do przetwarzania danych osobowych nadane pracownikom sprzątającym, a w ich miejsce wydane zostały zgody na przebywanie w obszarze przetwarzania danych osobowych, poza godzinami pracy Urzędu.

   (dowód: akta kontroli str. 223-226, 292-296, 301-305, 371-379, 381-387)

6. W Urzędzie od 1 stycznia 2017 r. do 11 stycznia 2018 r. nie był przeprowadzany okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji (ostatni przeprowadzono 9 września 2016 r.). Było to niezgodne z przepisem § 20 ust. 2 pkt 14 rozporządzenia KRI, w myśl którego bezpieczeństwo informacji realizowane jest poprzez zapewnienie przeprowadzenia audytu nie rzadziej niż raz na rok.

   Burmistrz wyjaśnił, że: *„Na skutek przeoczenia w 2017 roku audyt wewnętrzny z zakresu bezpieczeństwa informacji nie został przeprowadzony"*.

   (dowód: akta kontroli str. 204-220, 292-296)

7. Pracownikom zaangażowanym w proces przetwarzania informacji nie zapewniono szkoleń, które uwzględniałyby zagadnienia z zakresu zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji (odpowiedzialność karna), stosowanie środków zapewniających bezpieczeństwo informacji (m.in. urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich). Stanowiło to naruszenie § 20 ust. 2 pkt 6 rozporządzenia KRI, stosownie do którego zarządzanie bezpieczeństwem informacji realizowane jest przez zapewnienie szkolenia – obejmującego ww. zakres – osób zaangażowanych w proces przetwarzania informacji.

   Burmistrz wyjaśnił, że pracownicy Urzędu zostali objęci szkoleniem z zakresu ochrony danych osobowych, którego tematyka była opracowana przez firmę zewnętrzną. W wyniku mylnej interpretacji uznano, że odpowiada ona w pełni obowiązującym przepisom. (dowód: akta kontroli str. 219-220, 292-294, 393)

8. W obowiązującej w Urzędzie Polityce bezpieczeństwa nie uwzględniono części wymogów określonych w § 20 ust. 1 rozporządzenia KRI. Rozwiązania przyjęte w Polityce bezpieczeństwa i Instrukcji zarządzania dotyczyły jedynie ochrony danych

osobowych, nie regulowały natomiast całościowych procedur związanych z bezpieczeństwem informacji.

Burmistrz wyjaśnił, że: *„Na skutek niedopatrzenia Polityka bezpieczeństwa informacji nie została opracowana całościowo. W najbliższym czasie treść Polityki zostanie dostosowana do wymagań § 2 pkt 15 rozporządzenia KRI (...).*"

(dowód: akta kontroli str. 36-65, 219-220, 292-296)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działalność Urzędu dotyczącą opracowania i wdrożenia dokumentacji oraz procedur ochrony danych i zgłaszania rejestracji zbiorów do GIODO.

3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

3.1. W załączniku do Polityki bezpieczeństwa „Wykaz zabezpieczeń fizycznych, informatycznych oraz organizacyjnych" określony został sposób zabezpieczenia pomieszczeń Urzędu: [1] alarm przeciwwłamaniowy, [2] monitoring wizyjny, gaśnice, [3] rolety w oknach [4] kraty w oknach na parterze. W wyniku przeprowadzonych oględzin stwierdzono, że zastosowane zabezpieczenia były zgodne z założonymi. W Polityce bezpieczeństwa nie były określone dodatkowe wymagania dla pomieszczeń przeznaczonych na archiwum. W wyniku przeprowadzonych oględzin stwierdzono, że pomieszczenie archiwum zostało wyposażone w czujnik ruchu i wilgoci oraz gaśnicę.

(dowód: akta kontroli str. 29-35, 66, 92)

Polityka kluczy została uregulowana w pkt 8 ppkt 6 – 8 Polityki bezpieczeństwa, zgodnie z którym pomieszczenia, w których przetwarza się dane osobowe są zamykane na klucz w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych, zarówno po zakończeniu pracy, jak i w godzinach pracy. Klucze do pomieszczeń służbowych mogli pobierać wyłącznie wyznaczeni pracownicy (zgodnie z załącznikiem nr 12 do Polityki bezpieczeństwa *Wykaz kluczy do pomieszczeń, gdzie gromadzone są dane osobowe, wraz ze wskazaniem osób mogących je pobrać.* (dowód: akta kontroli str. 36-51, 66)

3.2. W Urzędzie prowadzona była ewidencja oprogramowania dopuszczonego do użytkowania oraz wykaz użytkowanego sprzętu komputerowego. Nie była ona jednak na bieżąco aktualizowana i nie obejmowała danych dotyczących systemów operacyjnych zainstalowanych na komputerach, a także danych dotyczących konfiguracji oprogramowania. Było to niezgodne z § 20 ust. 2 pkt. 2 rozporządzenia KRI, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 93, 99)

3.3. W okresie objętym kontrolą w Urzędzie nie dokonywano likwidacji sprzętu będącego nośnikiem danych. (dowód: akta kontroli str. 228-237)

3.4. Niszczenie dokumentów w Urzędzie, zgodnie z pkt 8 ppkt 12 Polityki bezpieczeństwa, odbywało się za pomocą niszczarek. Do tego celu Urząd wyposażono w sześć niszczarek. (dowód: akta kontroli str. 29-33, 36-51)

3.5. W Urzędzie z komputera przenośnego korzystał Skarbnik Gminy. Pracowników użytkujących komputery przenośne zobowiązano do zachowania szczególnej ostrożności podczas transportu, przechowywania i użytkowania poza obszarem przetwarzania danych oraz nieużytkowania ich w miejscach publicznych, a także niepozostawiania bez nadzoru bądź powierzania osobom nieuprawnionym. Pracownikom nie umożliwiono zdalnego dostępu do zasobów sieci lokalnej Urzędu. (dowód: akta kontroli str. 27-28, 46-53)

3.6. Sprzątanie pomieszczeń, w których przetwarzano dane osobowe odbywało się poza godzinami pracy Urzędu. Pracownicy sprzątający do 14 grudnia 2017 r. posiadali upoważnienia do przetwarzania danych osobowych, a nie zgody ADO na przebywanie w obszarze przetwarzania danych poza godzinami pracy Urzędu, (co szerzej opisano w pkt 2 wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości"). Sprzątanie pomieszczenia serwerowni odbywało się przez ASI.

Zgodnie z przyjętymi w Urzędzie uregulowaniami, dokumenty zawierające dane osobowe powinny być przechowywane w szafach zamykanych na klucz. Za prawidłowe

zabezpieczenie danych osobowych oraz miejsc ich przechowywania w trakcie i po zakończeniu pracy odpowiedzialni byli pracownicy upoważnieni do przetwarzania danych osobowych. Oględziny jedenastu pomieszczeń tworzących obszar, w którym przetwarzano dane osobowe wykazały, że w ośmiu dane osobowe nie były właściwie zabezpieczone, bowiem nie były przechowywane w zamkniętych szafach (szerzej opisano to w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości").

(dowód: akta kontroli str. 29-33, 36-51)

3.7. W Urzędzie były opracowane procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych. Zgodnie z pkt 10 Instrukcji zarządzania, osobą odpowiedzialną za wykonywanie przeglądów i konserwacji był ASI oraz KODO. Przeglądy systemów informatycznych powinny odbywać się przynajmniej raz w roku.

W okresie objętym kontrolą przeglądy i konserwacje nie były przeprowadzane, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 52-65, 219-220)

3.8. W Urzędzie nie były przygotowane rozwiązania na wypadek wystąpienia sytuacji nadzwyczajnych, np. awarii, długotrwałego braku zasilania, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności".

25 komputerów było zabezpieczonych przed utratą zasilania, za pomocą zasilaczy awaryjnych UPS. Nie zabezpieczono dwóch komputerów przeznaczonych do prostych prac biurowych. Serwerownię Urzędu wyposażono w UPS. W Urzędzie nie było opracowanych procedur dotyczących przywracania systemów po awarii oraz planu ciągłości działania umożliwiającego kontynuację wykonywania zadań publicznych. Opracowano natomiast sposób tworzenia i przywracania kopii zapasowych. Urząd posiadał dodatkowe źródło zasilania na wypadek długotrwałych przerw w dostawie prądu.

(dowód: akta kontroli str. 29-33, 219-220)

3.9. W Urzędzie od 1 stycznia 2016 r. do 1 grudnia 2017 r. nie wystąpiły przypadki fizycznej utraty danych. (dowód: akta kontroli str. 219-220)

Ustalone nieprawidłowości

W działalności jednostki w przedstawionym wyżej zakresie stwierdzono niżej wymienione nieprawidłowości.

1. Rejestr zasobów informatycznych w zakresie sprzętu i oprogramowania do przetwarzania informacji (który zawiera ich rodzaj i konfigurację) nie był prowadzony na bieżąco. Było to niezgodne z wymogami § 20 ust. 2 pkt 2 rozporządzenia KRI, stosownie do których zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

   ASI wyjaśnił, że: *„Prowadzony rejestr sprzętu i oprogramowania służącego do przetwarzania informacji będzie aktualizowany na bieżąco oraz zostanie uzupełniony"*. (dowód: akta kontroli str. 93, 99, 284-291)

2. W Urzędzie nie były przeprowadzane przeglądy i konserwacje systemów oraz nośników informacji służących do przetwarzania danych. Zgodnie z pkt 10 Instrukcji zarządzania, osobą odpowiedzialną za wykonywanie przeglądów i konserwacji był ASI oraz KODO, a przeglądy systemów informatycznych powinny odbywać się przynajmniej raz w roku. Zgodnie z § 20 ust. 2 pkt 12 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych.

   ASI wyjaśnił, że: *„Przeglądy i konserwacje systemów oraz nośników informacji służących do przetwarzania danych nie były wykonywane w 2016 r. z powodu braku czasu"*. (dowód: akta kontroli str. 52-65, 219-220, 300)

3. Oględziny pomieszczeń Urzędu tworzących obszar, w którym przetwarzano dane osobowe wykazały, że w ośmiu (z jedenastu) pomieszczeniach dokumenty zawierające dane osobowe nie były właściwie chronione przed dostępem osób nieuprawnionych.

Meble biurowe służące do ich przechowywanie nie były bowiem zamykane na klucz. Było to niezgodne z pkt 8 ppkt 8 – 10 Polityki bezpieczeństwa, stosownie do którego dane osobowe w wersji papierowej po zakończeniu pracy należało przechowywać w zamykanych na klucz meblach biurowych, a klucze powinny być zabezpieczone przed dostępem osób nieupoważnionych. Szafy z danymi powinny być otwierane na czas potrzebny na dostęp do danych, a następnie powinny być zamykane.

Burmistrz wyjaśnił, że: *„W dniu 13 grudnia 2017r została podpisana umowa z wykonawcą na przeprowadzenie remontu kapitalnego budynku Urzędu Miejskiego w Szepietowie. Remont zakłada między innymi wyposażenie pomieszczeń w szafy zamykane na klucz w których będą przechowywane wszystkie dokumenty zawierające dane osobowe, co pozwoli zapobiec istniejącej sytuacji przechowywania części dokumentów w otwartych regałach i szafach. Zakup szaf zamykanych na klucz wstrzymano w związku z trwającymi kilka lat przygotowaniami do generalnego budynku UM w Szepietowie".* (dowód: akta kontroli str. 29-33, 36-51, 292-296)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę na potrzebę opracowania w Urzędzie wewnętrznych regulacji na wypadek wystąpienia sytuacji nadzwyczajnych (np.: długotrwałego braku zasilania, przywracania systemów po awarii), a także planu ciągłości działania, umożliwiającego kontynuację wykonywania zadań jednostki. Plan ten powinien określić systemy i aplikacje o znaczeniu krytycznym oraz wszystkie podporządkowane lub powiązane plany. Istotne jest, aby plany te były jasno udokumentowane, przekazane pracownikom i aktualizowane w celu odzwierciedlenia bieżącej działalności Urzędu. Ponadto obowiązek zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej wynika z regulacji cz. A pkt III załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych.

Burmistrz wyjaśnił, że: *„Mylna interpretacja Instrukcji naruszenie bezpieczeństwa danych osobowych stanowiącej integralną część Polityki bezpieczeństwa stanowi przyczynę braku opracowania wewnętrznych regulacji dotyczących rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych np. długotrwałego braku zasilania bądź przywracania systemów po awarii, a także braku ciągłości działania umożliwiającego kontynuację wykonywania zadań jednostki".* (dowód: akta kontroli str. 219-220, 292-296)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działania Urzędu dotyczące przestrzegania przyjętych procedur w zakresie przechowywania i zabezpieczania danych, które nie zapewniały ich właściwej ochrony.

Opis stanu faktycznego

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności jednostki kontrolowanej

4.1. W Urzędzie prowadzono 41 zbiorów danych[10], w tym 33 w formie papierowej i osiem w formie elektronicznej. Do gromadzenia i przetwarzania danych wykorzystywano m.in. systemy: [1] Infosystem, w którym prowadzono zbiór *Podatki,* [2] ŹRÓDŁO i SelWin: *Rejestr mieszkańców, Rejestr zamieszkania cudzoziemców, Dowody osobiste, Akta stanu cywilnego, Rejestr wyborców;* [3] SmartDoc: *Rejestr korespondencji;* [4] CEIDG: *Działalność gospodarcza;* [5] *System kadrowo-płacowy;* [6] *Płatnik.* (dowód: akta kontroli str. 93)

4.2. W okresie objętym kontrolą nie dokonywano aktualizacji zbiorów danych zgłoszonych do GIODO. Na podstawie analizy pięciu zbiorów stwierdzono, że w dwóch zakres przetwarzanych danych był zgodny z danymi wskazanymi w zgłoszeniach do GIODO, a w pozostałych trzech przetwarzano dane w szerszym zakresie niż zgłoszono, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 250-267, 272-278)

4.3. We wszystkich objętych analizą zbiorach danych zakres gromadzonych i przetwarzanych danych osobowych był niezbędny do realizacji zadań, które zostały przypisane Urzędowi. (dowód: akta kontroli str. 272-278, 361-379)

[10] Jeden zbiór *Karta dużej rodziny* powierzono do prowadzenia Miejsko-Gminnemu Ośrodkowi Pomocy Społecznej.

Urząd wywiązał się z obowiązku poinformowania kandydatów do pracy o konieczności zawarcia w dokumentach aplikacyjnych klauzuli dotyczącej zgody na przetwarzanie danych osobowych do celów realizacji procesu rekrutacji, zgodnie z ustawą o ochronie danych osobowych. (dowód: akta kontroli str. 246-249)

4.4. Urząd posiadał dostęp do zewnętrznych zbiorów danych osobowych: ŹRÓDŁO i CEiDG. Dostęp do systemu ŹRÓDŁO uzyskał na podstawie upoważnienia z 28 listopada 2014 r. nadanego przez Ministra Spraw Wewnętrznych. Urząd spełnił wymogi związane z dostępem do tego systemu: dwa stanowiska komputerowe do obsługi systemu nie posiadały dostępu do Internetu, a pracownicy uzyskali stosowne upoważnienia. Dostęp do systemu CEiDG posiadało dwóch pracowników Urzędu, którzy uzyskali go na podstawie zgłoszenia z 17 czerwca 2011 r. do Ministerstwa Gospodarki.
(dowód: akta kontroli str. 168-174)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegająca na przetwarzaniu w trzech (z pięciu) zbiorach danych osobowych w zakresie szerszym niż wskazany w zgłoszeniach do GIODO. Przetwarzane dane obejmowały dodatkowo datę urodzenia, nr PESEL, imiona rodziców.

Burmistrz wyjaśnił to pomyłką. (dowód: akta kontroli str. 272-278, 292-296)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonej nieprawidłowości sposób przetwarzania zasobów informacyjnych, który był zgodny z zakresem działalności Urzędu, a w odniesieniu do zbiorów zewnętrznych spełniał wymogi związane z dostępem do tych zbiorów.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[11] wnosi o:

1. Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, a także przeglądów i konserwacji systemów informatycznych oraz nośników informacji służących do przetwarzania danych.
2. Niezwłoczne cofanie uprawnień dostępu do systemu w związku z ustaniem zatrudnienia, oraz podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych zadań oraz obowiązków.
3. Monitorowanie dostępu do zasobów informacyjnych Urzędu.
4. Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, w szczególności poprzez aktualizację oprogramowania.
5. Wykonywanie kopii bezpieczeństwa, zgodnie z pkt 6 – 8 Instrukcji zarządzania, oraz sprawdzanie zgodności ich wykonania.
6. Realizowanie przez ADO zadania w zakresie sprawdzania zgodności przetwarzanych w Urzędzie danych osobowych z przepisami o ich ochronie.
7. Uzupełnienie ewidencji osób upoważnionych do przetwarzania danych osobowych o zakres udzielonych upoważnień.
8. Przeprowadzanie nie rzadziej niż raz w roku okresowego audytu bezpieczeństwa informacji.
9. Zapewnienie pracownikom zaangażowanym w proces przetwarzania informacji szkoleń z zakresu zagrożenia bezpieczeństwa informacji.
10. Wprowadzenie regulacji stanowiących politykę bezpieczeństwa informacji, zgodnej z § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI.

[11] Dz. U. z 2015 r. poz. 1096 ze zm. Ustawa zwana dalej „ustawą o NIK".

11. Prowadzenie rejestru zasobów informatycznych, zgodnie z wymogami określonymi w § 20 ust. 2 pkt 2 rozporządzenia KRI.
12. Przechowywanie danych osobowych w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
13. Zaktualizowanie zbiorów danych zgłoszonych do GIODO.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden kierownikowi jednostki kontrolowanej, drugi do akt kontroli.

Zgodnie z art. 54 ustawy o NIK, kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Białymstoku.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK, proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Białystok, dnia 30 stycznia 2018 r.

Kontroler
Beata Palinowska
starszy inspektor kontroli państwowej

Palinowska Beata
podpis

DYREKTOR DELEGATURY
Najwyższej Izby Kontroli w Białymstoku
z up. WICEDYREKTOR
Robert Skwarko

podpis